Remarks

Reconsideration is requested in view of the preceding amendments and the following remarks. Claims 3, 5, 8-10, and 19 are in the application.

Claim 3 is amended to correct an obvious typographical error.

Claim 19 stands rejected as being directed to non-statutory subject matter. Withdrawal of this rejection is requested in view of the amendment to claim 19.

Claims 3, 5, 8, 10, and 19 stand rejected as anticipated by Shimbo, U.S. Patent 6,088,453 ("Shimbo"). This rejection is traversed. Claim 3 recites a computer readable medium that recites computer-executable instructions for a method that includes, in part, selecting a Montgomery radix $R = 2^m$, wherein m is an integer multiple of a wordsize, and m is greater than a bit-length of the prime number p and determining values (r, k) from an almost Montgomery inverse function. If k is less than m, then r is assigned a value obtained as a Montgomery product of r and R^2 mod p, and k is assigned a value $k = k + m$. Shimbo fails to teach or suggest such a method. Shimbo at col. 11, lines 27-35 is cited as teaching determining if $k < m$ and assigning k a value $k = k + m$ based on the determination. However, review of the cited portion of Shimbo shows that Shimbo teaches only that k is an integer greater than or equal to L and less than or equal to $2L$, wherein L is a number of bits in a modulus p. See Shimbo, col. 8, lines 19-22. Shimbo indicates that k is obtained by an inverse calculation unit, but does not teach determining if k is less than m or assigning k a value $k + m$ based on the determination. In view of Shimbo's failure to teach the feature for which it is cited, withdrawal of this rejection is requested.

Claims 5 recites a cryptographic system for encryption and decryption. The system comprises a module for transforming a message according to a method that includes, in part, selecting a Montgomery radix $R = 2^m$, wherein m is an integer multiple of a wordsize, and m is greater than a bit-length of the prime number p. Values (r, k) are determined from an almost Montgomery inverse function. If k is less than m, r is assigned a value obtained as a Montgomery product of r and R^2 mod p, and k is assigned a value $k = k + m$. Shimbo does not teach or suggest such a cryptographic system. As noted above, Shimbo at col. 11, lines 27-35 is cited as teaching determining if k is less than m and assigning k a value of $k + m$ based on the determination. However, the cited portion of Shimbo does not teach or suggest such a determination or an assignment of k. Withdrawal of the rejection is requested.

Claim 8 recites a cryptographic system having an encryption/decryption module that performs a method for obtaining a classical inverse of a message. The method comprises, in part, obtaining values (r,k) by calculating an almost Montgomery inverse function of a representation of a message using a Montgomery radix $R = 2^m$, wherein m is an integer multiple of a wordsize and is greater than a bit-length of a prime number p. If the value k is greater than m, then the value r is assigned a value equal to a Montgomery product of r and 1, and k is assigned a value of $k - m$. This rejection is traversed. Shimbo at col. 16, lines 46-53 and Fig. 12E (steps S827, S828) are cited as teaching assigning k a value of $k - m$. This is incorrect. Shimbo teaches decrementing a value T by p, wherein p is a prime modulus. In contrast, claim 8 recites decrementing a value k by an integer multiple of a wordsize, i.e., by a non-prime number that is not a prime modulus. In addition, Shimbo's inverse calculation unit 301 provides values $A^{-1}2^k$ mod p and k, and the value T is associated with a calculation result for $A^{-1}2^k$ mod p, not the

value k. Shimbo, col. 11, lines 28-30 and col. 12, lines 38-39. For at least these reasons, claim 8 and dependent claim 9 are properly allowable.

Claim 10 recites a computer-readable medium, comprising instructions for performing a method for obtaining a classical inverse of a message. The method comprises, in part, obtaining values (r,k) by calculating an almost Montgomery inverse function of a representation of a message using a Montgomery radix $R = 2^m$, wherein m is an integer multiple of a wordsize and is greater than a bit-length of a prime number p. If k is greater than m, then r is assigned a value equal to a Montgomery product of r and 1, and k is assigned a value of $k - m$. As noted above, the cited portions of Shimbo fail to teach or suggest such a method. In particular, Shimbo fails to teach or suggest decrementing a value k by an integer multiple of a wordsize, i.e., by a non-prime number that is not a prime modulus. Accordingly, claim 10 is properly allowable.

Claim 19 recites a computer-readable medium containing instructions for performing a method for computing a multiplicative inverse of an M-residue $A = a2^m \bmod p$, wherein p is a prime number, m is an integer, and a Montgomery radix $R = 2^m$. The method comprises, in part, computing an intermediate product r and an integer k using an almost Montgomery inverse procedure, and determining if k is less than or equal to m. If so, k is assigned a value of $k + m$. Shimbo fails to teach such computer readable medium. As noted above, the cited portions of Shimbo do not teach or suggest determining if k is less than or equal to m, or assigning k a value of $k + m$ based on the determination. Accordingly, claim 19 is properly allowable.

Claim 9 stands rejected as allegedly obvious from a combination of Shimbo and Kobayahi et al., U.S. Patent 6,795,553. This rejection is traversed. Claim 9 is properly allowable as dependent from allowable claim 8.

In view of the preceding amendments and remarks, all pending claims are in condition for allowance and action to such end is respectfully requested.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

By _____
Michael D. Jones
Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 595-5300
Facsimile: (503) 228-9446